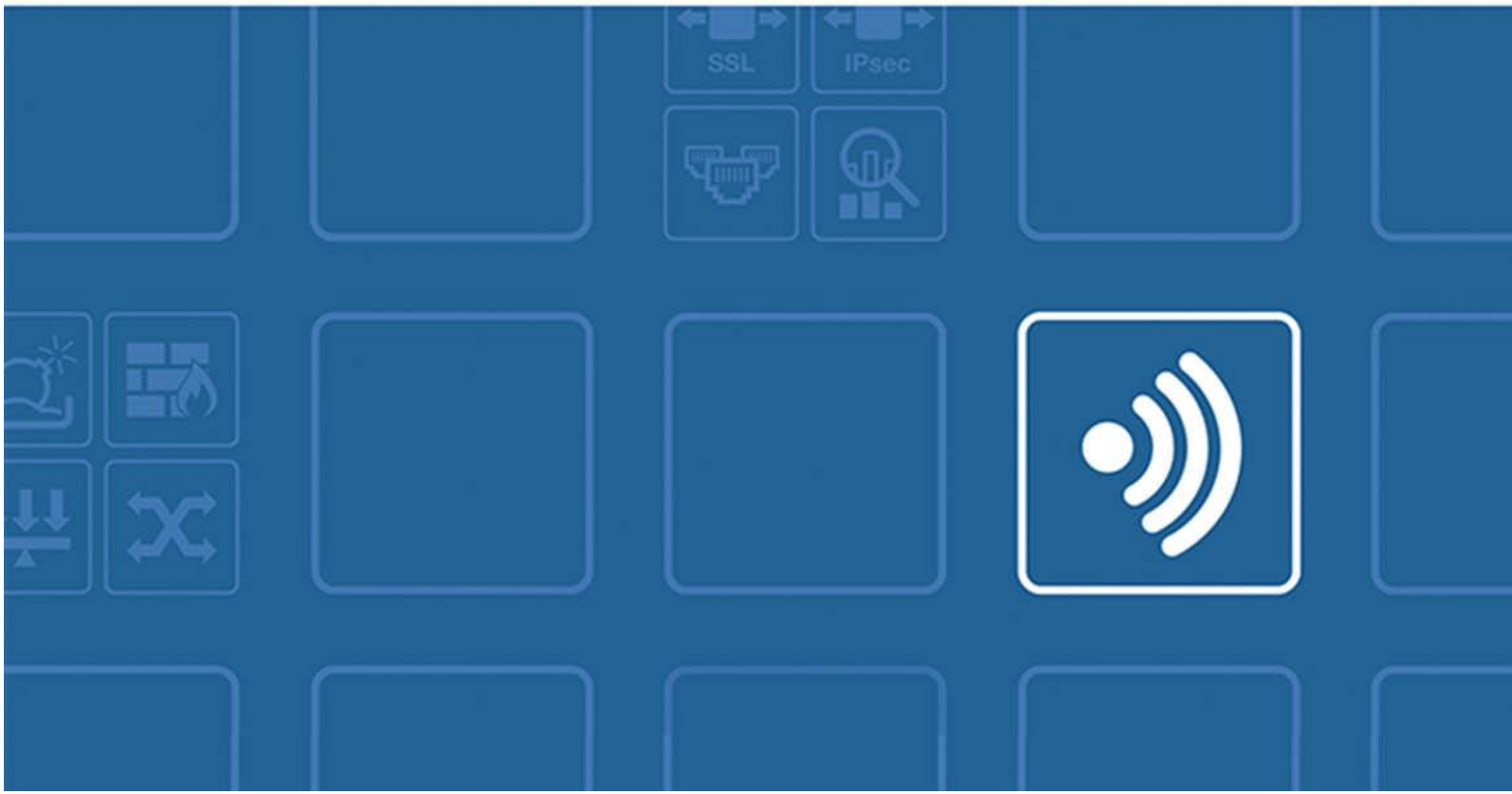
FORTINET
High Performance Network Security

FortiWLC (SD)

Release 8.2.7MR



FortiWLC (SD) 8.2.7MR includes significant performance improvements for FAPU42x series access points, DFS certification (FCC, CE, Korea, and Japan), and fixes for security vulnerability issues. In addition, various fixes and enhancements are available as listed in the Fixed Issues section.

Support for 802.3af and 802.3at for FAP

In addition, this release supports 802.3af and 802.3at power supply for FAP-U421 and FAP-U423. When connected to **802.3af power**, the following is the expected behaviour.

- FAPs powered using **802.3af power**, will boot up and will operate in *2x2 MIMO mode* with 17dbm transmit power. The USB port will be disabled on these FAPs.
- FAPs powered using 802.3at, will continue to operate in the configured mode with default transmit power.
- Alarms are not generated when FAP is powered using 802.3af power supply.

To ensure a secured WiFi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Getting Started with Upgrade

Controller upgrade is performed via CLI interface. You will require a serial or SSH2 connection to connect to controller and use its CLI.

The following flowchart illustrates the approved upgrade path.

Supported Upgrade Releases

Release	GoTo Release Numbers
7.0	7.0-10-0
8.0	8.0-5-0, 8.0-6-0
8.1	8.1-3-2
8.2	8.2-4-0

Check Available Free Space

Total free space required is the size of the image + 50MB (approximately 230 MB). You can use the **`show file systems`** command to verify the current disk usage.

```
controller# show file systems
Filesystem 1K-blocks Used   Available Use% Mounted on
/dev/hdc2  428972    227844 178242    57%  /
none       4880      56     4824      2%   /dev/shm
none       19528     1788   17740     10%  /opt/meru/var/run
none       9764      240    9524      3%   /opt/meru/var/log
none       9764      68     9696      1%   /tmp
none       9764      0      9764      0%   /opt/meru/capture
```

The first partition (in the above example, /hdc2, although the actual name will vary depending on the version of FortiWLC-SD installed on the controller) is the one that must have ample free space.

In the example above, the partition shows 178242KB of free space (shown bolded above), which translates to approximately 178MB. If your system does not have at least 230MB (230000KB) free, use the **`delete flash:<flash>`** command to free up space by deleting older flash files until there is enough space to perform the upgrade (on some controllers, this may require deleting the flash file for the current running version).

Set up Serial Connection

Ensure that your serial connection is set for the following options:

Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

- Baud--115200
- Data--8 bits
- Parity--None
- Stop Bit—1
- Flow Control—None

Supported Hardware and Software

Hardware and Software	Supported		Unsupported
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e AP332e, AP332i* AP433e, AP433i, OAP433e* FAP U421EV FAP U423EV	AP1010e, AP1010i* AP1020e, AP1020i* AP1014i* AP110* AP822 PSM3x*	AP201 AP208 AP150 AP300, AP301, AP302, AP302i, AP301i AP310, AP311, AP320, AP310i, AP320i OAP180 OAP380
*Cannot be configured as a relay AP			
Controllers	FortiWLC 50D FortiWLC 200D FortiWLC 500D		MC 5000 MC 4100 MC 1500

Hardware and Software	Supported	Unsupported
	MC6000 MC4200 (with or without 10G Module) MC4200-VE MC3200 MC3200-VE MC1550 MC1550-VE	MC 1500-VE
FortiWLM	8.3.0	
FortiConnect	15.10	
Browsers		
FortiWLC (SD) WebUI	Internet Explorer 9,10 Mozilla Firefox 25+ Google Chrome 31+	
 A limitation of Firefox 3.0 and 3.5+ prevents display of the X-axis legend of dashboard graphs.		
Captive Portal	Internet Explorer 6, 7, 8, 9, 10, IE11 and Edge. Apple Safari Google Chrome Mozilla Firefox 4.x and earlier Mobile devices (such as Apple iPhone and BlackBerry)	

Upgrading

- Virtual cell across Wave1 and Wave2 AP is supported.

1. Download image files from an FTP or TFTP server to the controller using one of the following commands:

```
# copy ftp://ftpuser:<password@ext-ip-addr>/<?-release-version>-MC_MODEL-rpm.tar<space>.
or
# copy tftp://<ext-ip-addr>/<?-release-version>-MC_MODEL-rpm.tar<space>.
```

? in *<release-version>* is suffixed with meru for MC devices and forti for FWLC devices.

2. Disable AP auto upgrade and then upgrade the controller

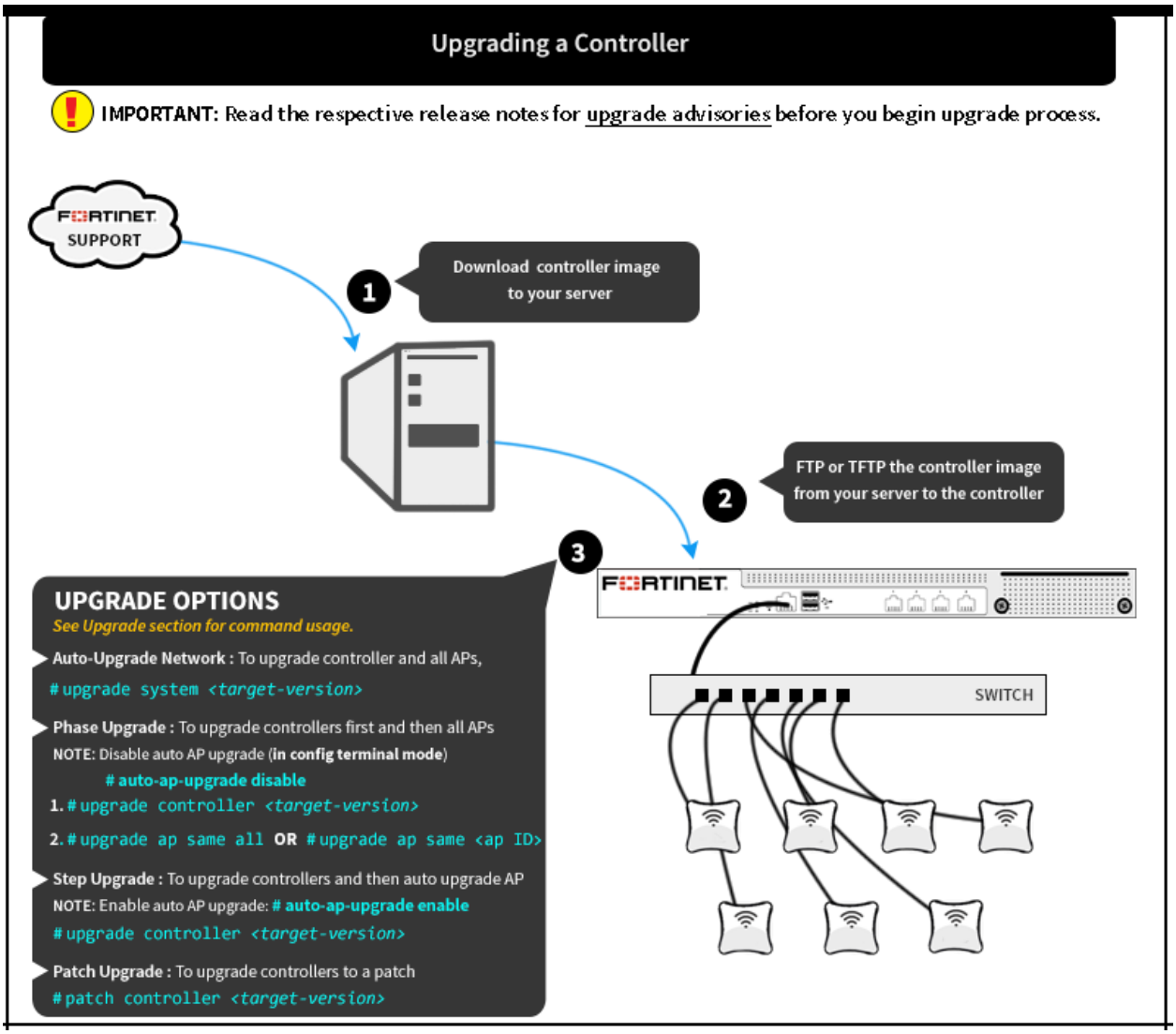
```
# configure terminal
# auto-ap-upgrade disable
# copy running-config startup-config
# upgrade controller <target version>
```

3. Upgrade the APs

```
# upgrade ap same all
```

After the APs are up, use the `show controller` and `show ap` command to ensure that the controller and APs are upgraded to the latest (upgraded) version. Ensure that the system configuration is

available in the controller using the `show running-config` command (if not, recover from the remote location). See the Backup Running Configuration step.



Upgrading an N+1 Site

To upgrade a site running N+1, all controllers must be on the same FortiWLC-SD version and the backup controller must be in the same subnet as the primary controllers. You can choose any of the following options to upgrade:

Option 1 - Just like you would upgrade any controller, you can upgrade an N+1 controller.

1. Upgrade master and then upgrade slave.
2. After upgrade, enable master on slave using the `nplus1 enable` command.

Option 2 - Upgrade slave and then upgrade master.

After upgrade, enable master service on slave using the `nplus1 enable` command.

Option 3 - If there are multiple master controllers

1. Upgrade all master controllers followed by slave controllers. After upgrade, enable all master controllers on slave controllers using the `nplus1 enable` command.
2. To enable master controller on slave controller, use the `nplus1 enable` command.
3. Connect to all controllers using SSH or a serial cable.
4. Use the `show nplus1` command to verify if the slave and master controllers are in the cluster. The output should display the following information:

```
Admin: Enable
Switch: Yes
Reason: -
SW Version: 8.2-6MR
```

5. If the configuration does not display the above settings, use the `nplus1 enable <master-controller-ip>` command to complete the configuration.
6. To add any missing master controller to the cluster, use the `nplus1 add master` command.

Restore Saved Configuration

1. Copy the backup configuration back to the controller:

```
# copy ftp://<user>:<passswd>@<offbox-ip-address>/runningconfig.txt orig-config.txt
```

2. Copy the saved configuration file to the running configuration file:

```
# copy orig-config.txt running-config
```

3. Save the running configuration to the start-up configuration:

```
# copy running-config startup-config
```

Upgrade Advisories

The following are upgrade advisories to consider before you begin upgrading your network.

Devices with Intel Chipset 62xx

Wireless devices with Intel chipset 62xx series must upgrade its firmware to version 18.20.x.x.

Mesh Deployments

When attempting to upgrade a mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller. *Be sure to disable the auto-ap-upgrade feature when performing this task*. The following procedure is recommended for optimal operation:

1. Disable the **`auto-ap-upgrade`** feature.
2. Copy the running-config to startup-config.
3. Upgrade the APs manually using `upgrade ap same all` command.

In order to prevent IP assignment problems after the upgrade, if your network utilizes VLAN configurations, ensure that the DHCP Relay Pass-through option is enabled in the following two locations:

- **Configuration** > **Devices**: *Controller*
- **Configuration** > **Wired**: *VLAN* > [Select VLAN]

Captive Portal and Fortinet Connect Deployment Recommendations

DNS Entry

It is mandatory to enter the DNS while creating internal DHCP profile.

External Portal IP Configuration:

If a NAT device is located between the controller and the Fortinet Connect, the IP address with which Fortinet Connect sees the controller should be configured under Device > RADIUS Clients page in Fortinet Connect Admin portal (*http://<fortinetconnect-ip-address>/admin*), . Select the RADIUS client and enter the controller IP address in the Client tab. The Fortinet Connect Automatic Setup then configures the controller correctly and ensures that the correct controller IP address is configured on Fortinet Connect.

Remember Me settings

In the Portal Settings step of the Guest Portal configuration wizard, if you choose to enable Remember Credentials, then select "Initially attempt to use a cookie, if that fails try the MAC address" option. This removes dependency on the client's browser and security settings.

SmartConnect Certificate download

In the Certificates step of the Smart Connect Profile Wizard, ensure that you select the complete certificate chain of your uploaded certificate. If you have uploaded all certificates in the chain (from root to server), then selecting the server certificate will automatically select the entire certificate chain.

- To upload the server certificates, goto **Server** > **SSL Settings** > **Server Certificate** tab.
- To upload rest of the chain, goto **Server** > **SSL Settings** > **Trusted CA Certificates** tab.

Chromecast Discovery

To ensure a Chromecast device receives packet from a client (publisher), both, the Chromecast device and the client must be in the same subnet. This is applicable to Chromecast version 1 and version 2.

CNA Bypass for Android 5.0 +

Devices running Android 5.0 and above introduces system default CP login pop-up windows. To disable this pop-up window enable CNA bypass in the controller.

In the WebUI

Go to **Configuration** > **Security** > **Captive Portal** > Advanced Settings section, select Captive Portal Prole and set **Apple Captive Network Assistant (CNA) Bypass** to **ON**.

Using CLI

Use the **ssl-server cna-bypass ON** command in config mode.

Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all APs or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, go to **Configuration** > **Devices** > **System Settings** > **Scale Settings** tab.
2. Enter a channel number in the *Voice Scale Channel List* field and click **OK**.

Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and these results in a noticeable reduction of throughput in data traffic.

IP Prefix Validation

In a situation where a station with an IP address from a different subnet connects to the controller, it can result in various network issues including outage. A new field, IP Prefix Validation is added to the ***ESS Profile*** and ***Port Profile*** configuration page. When enabled, stations with different subnet are prevented from connecting to the controller. By default, IP Prefix Validation in **ESS Profile is ON** and in **Port Profile it is OFF**.

QoS Rules

QoS rules with no matching criteria when *Match* is checked will abort an upgrade. To prevent this, check QoS rules to ensure that at least one matching criteria is set for each rule if *Match* is set.

Downgrade Procedure

Any controller that has been upgraded to 8.2-6 can only be downgraded to the previous release from which it was originally upgraded.

Obtain a signed image file for a downgrade from the FTP site and install it on the controller before the downgrading. To downgrade to an earlier release, use the upgrade procedure. Before downgrading to any release, save your configuration to a backup file and store it on a server accessible by FTP. The saved configuration can then be used to restore your configured parameters if needed. There are two upgrade command options.

You can upgrade the controller first using the **upgrade controller** command and then upgrade APs using the **upgrade ap same all** command. You can also use the **upgrade system** command; this downgrades the APs first, then the controller.

Fixed Issues

Bug ID	Description
350698	Fixed timeout issues during the keep-alive period in bridge mode.
353273	Fixed: AP1000 CPU goes to 0%, and AP stops transferring data with single client setup
373754	Fixed output of **show statistics ap-general** command.
377349	Fixed authentication issues with Motorola MC3000 devices.
378696	Fixed kernel crash issues on controllers running in 8.1-2-0
381029	Fixed SecurityMM crash that prevents WebUI login.
382927	Clients connected on the GRE-Profile mapped ESS can renew IP address.
383337	Fixed issues that resulted in incorrect CP page for internal CP users on bridge profile.
387680	Fixed issues that caused kernel crashes on a 500D controller running in 8.1-2-0.
390656	Fixed random controller reboots that resulted in kernel crash in 8.1-2-0.
391047	Fixed issues that prevented clients with Broadcom BCM943228Z to connect to the network.
392401	Ping from a VLAN is now available.
392411	Local admin login credentials are now encrypted in the running-config.
395009	Fixed random client disconnections.
397318	Fixed AP TX freeze after Uptime of 99 days.
398050	Fixed issues the resulted in client disconnections after Security MM restart.
406739	Fixed OAP832 power class value.
407596	Fixed issues that resulted in controller redirecting to https instead of HTTP for CP profiles
407897	Fixed client connections issues that occurred after SMM restart.
388249	The pam.log file is excluded from the diagnostics.
404249	Fixed issues causing config loss after upgrading from 8.1-2-0 to 8.3-0. This was noticed when the PSK contained special characters.
395994	Added fixes to prevent local Admin login credentials showing up in CLEAR TEXT in startup-config.
345126	In a N+1 set up, users can now view startup-config of a specific master controller using the `show nplus1 startup-config <ip of the master>` command.

Bug ID	Description
400555	Fixed TCP retries issues on port 8009.
407650	Fixed ping loss issues that affected some Marvel clients.
409415	Fixed AP reboots issues that were seen at "*NIP [c0255cbc] skb_pull+0x2c/0x40 LR [d3945180] mtunnel_packet_l2_rcv+0x4a8/0x1388 [meru_tunnel]*". The issue affected AP832e, AP822e, and AP832i
384645	Fixed throughput issues that affected clients with Marvel chipsets.
412646	Fixed MIB compilation issues that affected FortiWLC models.
415474	Mesh VLAN trunk works as expected for OAP832.
412419	Fixed issues that caused malformed JASON data. The issue was seen in AP822 and AP832 running SD 7.0.10
413746	Fixed *hostapd* process crash issues. This issue affected controllers running SD 7.0-9-1.
394663	Fixed incorrect VLAN assignment issues.
393292	Hardcoded core account has been removed.
393924	Fixed various issues that caused controller reboot.
386327	Fixed AP reboot uses seen with "*NIP: d3fa654c LR: d417de14 CTR: c00baa24*". This issue affected AP832 running 8.1.2.0
377253	Fixed issues that resulted in COA failures.
400676	Fixed incorrect AP Id issues.
388397	Removed hardcoded default password for ***rsync***.
387851	Fixed the issue of FortiWLC 500D controller reporting false alarms on power failure.

Common Vulnerabilities and Exposures

FortiWLC 8.2.7MR is no longer vulnerable to the following CVE-Reference:

- 2017-3134
- Visit https://fortiguard.com/psirt for more information

Known Issues

Bug ID	Description
414602	Downlink multicast traffic results in AP crashing with "epc : 80215b58 netif_r".

Bug ID	Description
	Workaround: Enable IGMP snooping in tunnel mode.
410454	Apple MacBook running OS X version 10.8.5, asks for username and password instead of passphrase when configured with WPA-PSK.
400651	Round trip time for ICMP echo/request-response between STAP and AP822 is longer than expected.
394554	Clients connected to a bridge mode profile are unable to switch back to bridge mode after they switched to a tunnel mode profile. Issue is noticed with AP832.
389852	The *mdebug.log* file size increases and fills `/var/log` up to 100%.
377891	DPI policy does not block *WhatsApp* traffic.
351641	There are known issues that result in leaf node AP to reboot with *LOST CONTACT with controller* error.
388882	There are known issues that result in the controller reporting incorrect number of stations.
377362	There are known issues that occasionally cause authentication failures when an external captive portal is used.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service